Single Rulebook Q&A

Question ID	2019_4826
Status	Final Q&A
Legal act	Directive 2015/2366/EU (PSD2)
Topic	Strong customer authentication and common and secure communication (incl. access)
Article	98
Paragraph	1
Subparagraph	d
COM Delegated or Implementing Acts/RTS/ITS/GLs/Recommendations	Regulation (EU) 2018/389 - RTS on strong customer authentication and secure communication
Article/Paragraph	33/ 4 and 5
Date of submission	12/07/2019
Published as Final Q&A	19/06/2020
Disclose name of institution / entity	No
Type of submitter	Competent authority
Subject matter	Scope of contingency mechanism
Question	Should the interfaces – referred to in Article 33(4) of the RTS - be interpreted to include not only the internet banking interface of the account servicing payment service provider (ASPSP) but also its proprietary mobile banking interface?
Background on the question	The access of the TPP to the contingency mechanism referred to in Article 33(4) of the RTS on SCA & CSC, provided the requirements set out in points (a) to (e) of Article 33 (5) of the RTS on SCA & CSC are adhered to, has long been assumed by ASPSPs to technically constitute screen scraping with identification of the online internet banking interface, i.e. the browser-based interface.There is however also a possibility to access payment accounts held with a specific ASPSP through the same channel as the one used by the ASPSP's proprietary mobile banking application and that ASPSP's back-end IT system. This proprietary mobile banking application of the ASPSP is indeed also an interface made available to the payment service users for the authentication and communication with their ASPSP.The question is now raised as to the form that the contingency mechanism should take, and more specifically whether the

	contingency mechanism should only take the form of a technique allowing access to the online internet banking interface of an ASPSP (such as the screen scraping with identification technique) or whether it could also take the form of a technique allowing the access of an ASPSP' proprietary mobile banking interface and the ways in which it communicates with the ASPSP's IT back-end?This question raises important issues about EU law beyond PSD2. After all the use of a technique allowing access to the ASPSP' proprietary mobile banking interface could constitute a breach of 1) rules against computer hacking laws (such as, for instance, the Directive 2009/24/EC on the legal protection of computer programs, which may apply in case of decompilation of software), 2) rules against cyber-crimes (such as, for instance, Directive 2013/40/EU on attacks against information systems), or 3) intellectual property rights. To conclude that such a technique were to be allowed, without adding the caveat that it should not constitute a breach of any of the above EU laws, would be too blunt a statement.In our view, this technique of accessing an ASPSP' proprietary mobile banking interface allows for the circumvention of the application of strong customer authentication by the ASPSP. The TPP essentially requests the PSU to enroll a second instance of the ASPSP' mobile application not on a phone under the PSU's control (possession) but on a server owned by the TPP. It is then the TPP that selects the password or PIN code to gain access to the mobile application and not the PSU. Coupled with an amount of code decompilation and reconstitution this allows the TPP to emulate the interaction between the ASPSP' mobile application and the ASPSP' IT back end.Hence the strong customer authentication that was in place through the mobile channel (possession of phone and mobile application + knowledge of PIN/password) is now entirely replaced by what is in the possession of the TPP (mobile application + PIN/password). This allows for the TPP to have continued access to all payment (and non-payment) accounts held by the PSU and to initiate payments without the PSU being involved. Hence this technique allows for the circumvention of the requirement imposed on ASPSPs to apply strong customer authentication under Article 97 of the PSD2.
EBA answer	Article 33(4) of the Commission Delegated Regulation (EU) 2018/389 provides that "As part of a contingency mechanism, payment service providers referred to in Article 30(1) shall be allowed to make use of the interfaces made available to the payment service users (PSUs) for the authentication and communication with their account servicing payment service provider (ASPSP), until the dedicated interface is restored to the level of availability and performance provided for in Article 32". Article 33(4) of the Delegated Regulation refers to "interfaces", in plural, and does not restrict the number of the PSU interfaces that third party providers (TPPs) are allowed to use as part of the contingency mechanism. It follows from the above that ASPSPs should allow TPPs, as part of the

	contingency mechanism in Article 33(4) of the Delegated Regulation, to use all interfaces made available by the ASPSP to its PSUs for accessing their payment accounts online directly. This includes not only the ASPSP's internet banking interface, but also the ASPSP's mobile banking application made available by the ASPSP to its PSUs, where applicable. The latter does not however imply that TPPs have an automatic right to access the ASPSP's proprietary mobile banking interface that connects the ASPSP's mobile banking app to the ASPSPs' backend systems. It is the ASPSP's responsibility to ensure that TPPs can be identified and can rely on the authentication procedures provided by the ASPSP to its PSUs, in accordance with the requirements of PSD2 and the Delegated Regulation. The above is in line with the underlying objective of the contingency mechanism, which is to ensure that TPPs can continue to provide their services in accordance with the Directive (EU) 2015/2366 (PSD2) and the Delegated Regulation in the event the dedicated interface is deficient, and is also supported by Article 28(2) of the Delegated Regulation which refers to "mobile applications and other payment services users' interfaces". Furthermore, TPPs accessing the PSUs' payment accounts using the contingency mechanism in Article 33(4) of the Delegated Regulation should also comply with their respective obligations under Article 33(5) of the Delegated Regulation, as well as with any other applicable EU legislation. In particular, the access by TPPs via the PSU interface(s) should not be used as a way of circumventing the application of strong customer authentication by the ASPSP.
Link	https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4826

European Banking Authority, 11/08/2020
www.eba.europa.eu